IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH "wildbilk" THAT IS STORED AT PREMISES CONTROLLED BY KIK C/O MEDIALAB.AI INC.	Case No. 3:22-mj-41

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Jonathan Funk, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Kik account that is stored at premises owned, maintained, controlled, or operated by Kik c/o MediaLab.ai Inc. (hereinafter "Kik"), an electronic communications service and/or remote computing service provider headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Kik to disclose to the government copies of the information (including the content of communications) described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI), currently assigned to HSI Harrisonburg, VA. I have been employed since September 2020. As part of my daily duties as an HSI Special Agent, I

investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251(a), 2252(a) and 2252A(a). I have received training in child pornography, child exploitation, and undercover chat investigations and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

3. I have participated in investigations of persons suspected of violating federal child pornography laws, including Title 18, United States Code, Sections 2422, 2251, 2252 and 2252A. These investigations have included the use of surveillance techniques, interviewing of subjects and witnesses, and planning and execution of arrest, search, and seizure warrants. In the course of these investigations, I have reviewed still images and videos containing child pornography and images depicting minor children engaged in sexually explicit conduct on various forms of electronic media including computers, digital cameras, and wireless telephones, and have discussed and reviewed these materials with other law enforcement officers. I have also participated in training programs for the investigation and enforcement of child pornography laws relating to the use of computers for receiving, transmitting, and storing child pornography. I have also been involved in trainings and investigations dealing with individuals soliciting and enticing minors through the use of computers.

4. This affidavit is based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the circumstances described herein, and a review of open-source information. This affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, and therefore does not include every fact

I have learned during the course of this investigation.

5. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Kik to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the account referenced in this affidavit and further in Attachment A, including the contents of the communications.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of violations of 18 U.S.C. § 2422(b) (attempted coercion and enticement of a minor to engage in illegal sexual activity) and 18 U.S.C. § 1470 (attempted transfer of obscene material to a minor) have been committed by an individual utilizing Kik account "**wildbilk"**. There is also probable cause to search the information described in Attachment A for evidence of these crimes, and contraband or fruits of these crimes, as described in Attachment B. Accordingly, I submit this application and affidavit in support of a search warrant authorizing a search of the Kik account "**wildbilk"**, as further described in Attachments A and B, incorporated herein by reference.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court of the Western District of Virginia is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

8. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual

depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

9. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

10. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

11. The term "computer," as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

12. The term "child erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

13. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT, RECEIVE OR DISTRIBUTE CHILD PORNOGRAPHY

14. Based on my previous experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

a. Individuals who have sexual discussions with minors and request images from minors may seek a virtual or actual sexual relationship with a minor through the internet and may have child pornography on electronic devices owned/possessed by them.

b. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

c. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their

own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

d. Likewise, individuals with intent to view and/or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Individuals who coerce and entice minors may use alcohol and/or narcotics to lower the inhibitions of children they are attempting to seduce.

BACKGROUND ON KIK

15. Kik advertises itself as "the first smartphone messenger with a built-in browser." Kik Messenger allows its users to "talk to your friends and browse and share any web site with your friends on Kik." According to the website, Kik Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat experience you can get on a smartphone. Unlike other messengers, Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control with whom they communicate. In addition, Kik features include more than instant messaging. Kik users can exchange images,

videos, sketches, stickers and even more with mobile web pages.

16. The Kik application (app) is available for download via the App Store for most iOS devices such as iPhones and iPads. Additionally, the Kik app is available on the Google PlayStore for Android devices. Kik can be used on multiple mobile devices, to include cellular phones and tablets.

17. In general, providers like Kik ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address.

18. An Electronic Service Provider (ESP), like Kik, typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, ESPs often have records of the Internet Protocol address (IP address) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

19. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems or complaints from other users. Providers typically retain records about such communications, including records of e-mails and other contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

20. Information stored at Kik, including that described above, may provide crucial evidence of the details and methodology of the criminal conduct under investigation. In my training and experience, the data pertaining to an account that is retained by a provider like Kik can also indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up and other communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a Kik account at a relevant time. Further, such stored electronic data can show how and when the account was accessed or used. Such "timeline" information allows investigators to understand the chronological context of the usage of a Kik account, account access, and events relating to the crime under investigation. Additionally, stored electronic data may provide relevant insight into the state of mind of the user of a Kik account as it relates to the offense under investigation. For example, information relating to a particular Kik account may indicate the user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

21. Kik offers users the ability to create an identity within the app referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is displayed in their Kik profile.

22. Kik maintains certain content data that is uploaded and shared by users including images and videos associated to the Kik account, a log showing the usernames that Kik account

added and/or blocked, and abuse reports associated with the Kik account.

23. Kik users are also able to create chat groups of up to 50 people to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the group. Once the group is created, Kik users can share a link to the group with any other Kik user.

24. Kik also retains data in regards to groups to which a user belongs. That data includes: information logs (containing the group name(s), group type, and the status of the group that a user belongs to); create logs (containing the details about who created the group and at what time); join logs (containing the timestamps and the method of users who have joined the group); leave logs (containing the timestamps and the method of users who have left the group); transactional chat log (containing a log of all the messages that a group has received, including sender username, timestamps, IP of the sender, receiver username(s), and word count, but not the actual message that was sent); chat platform log (containing a log of all the media files that a group received, including sender username, timestamps, IPs of the sender, receiver username(s), media type, and content ID); photographs and/or videos received by the group; and group abuse reports (containing a transcript of reported chat history against the subject group, including sender username, receiver username, timestamps, actual message, and content IDs).

PROBABLE CAUSE

25. On February 22, 2021, Undercover Detectives (UC) with the Albemarle County Police Department (ACPD), along with Homeland Security Investigations (HSI) Special Agent (SA), were online portraying themselves as a 14-year-old girl as part of an undercover chat operation involving individuals using the internet to sexually exploit children and those trafficking and soliciting children for commercial sex acts. The UC was using the undercover name of

"Ashley." While on Kik, UC was approached by a male with the name "Bill Prince" (later identified as William PRICE), whose username was "wildbilk" who stated he was 63 years old. During the conversation, the UC informed PRICE she was "almost" 15 years old. Undeterred, PRICE continued to chat with the UC.[1]

26. At one point in the beginning of the chat, PRICE stated "I probably shouldn't be chatting with you" implying he knew he should not be conversing or chatting with "Ashley" given her age. The chat became sexual in nature. PRICE asked the UC if she was a virgin. Later during the conversation, PRICE sent Ashley a photograph of his penis and asked Ashley if she wanted "to stroke it." PRICE soon after sent a series of unsolicited videos where he was masturbating saying "Oh Ashley… oh yes… it feels so good." (Ashley was the name the UC was using for the 14-year-old girl).

27. On or about February 24, 2021, PRICE renewed his conversation with the UC. During this round of conversations, in describing what he would like to do with the UC, PRICE explained "I'd let you ride my mouth while I stroke your nipples."

28. Weeks later, PRICE asked the UC if he could watch her get ready for school. PRICE then asked for the UC to send him a picture of her. When asked what type of picture the UC should send, PRICE responded, "I'd love to see you topless."

29. In March 2021, Kik responded to the summons ICE-HSI-HH-2021-00027 with the following information: Username "wildbilk" (Bill Prince) opened the account on August 8, 2018 utilizing email billprice0052005@yahoo.com.

---

[1] The UC communicated with username "wildbilk" while located in the Albemarle County Police Department in the Western District of Virginia.

30. In April 2021, Kik responded to the summons ICE-HSI-HH-2021-00037 with the following information: Username "wildbilk" (Bill Prince) opened the account on August 8, 2018 utilizing email billprice0052005@yahoo.com.

31. In March 2022, PRICE renewed discussions with the UC.

32. PRICE was still using his Kik account that the earlier communications took place on. PRICE had updated his profile picture since the last chat took place. The UC was online portraying himself as a now 15-year-old girl (Ashley) since it had been a year from the last communication with PRICE. PRICE still had his Kik name labeled as Bill Prince and a username of "wildbilk" and now stated he was 64 years of age. All information is consistent with previous communication with PRICE. During this chat session the UC advised PRICE that Ashley's current age was 15 years old. PRICE continued to chat with UC even after being advised of the UC's age. The chat, again, became sexual in nature.

33. For example, during the chat, PRICE instructed Ashley to "squeeze and stroke" her nipples. PRICE then asked Ashley if she wanted to play with his penis and then sent Ashley an unsolicited picture and video of his erect penis.

34. In April 2022, in response to legal process, Kik again affirmed that the "wildbilk" username belonged to an individual named Bill Prince and was registered to the following email address: billprice0052005@yahoo.com.

35. In general, providers like Kik ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number).

36. Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

37. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

38. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Kik to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

REQUEST FOR SEALING

39. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

CONCLUSION

40. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to require Kik, and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to Kik with direction that they identify the account described in Attachment A to this affidavit, as well as other subscriber, log, and content records associated with the account, as set forth in Section I of Attachment B to this affidavit. The search warrant will direct Kik to create an exact copy of the specified account and records.

41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Kik. Because the warrant will be served on Kik, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

42. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data and identify from among that content those items that come within the items identified in Section II to Attachment B for seizure.

43. Analyzing the data contained in the forensic copy may require special technical skills, equipment, and software, and it may be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

44. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2422(b) (attempted coercion and enticement of a minor to engage in illegal sexual activity) and 18 U.S.C. § 1470 (attempted transfer of obscene material to a minor) are located in the Kik account "**wildbilk"**, as more fully described in Attachments A and B to this Affidavit. I therefore request that the court issue a warrant authorizing a search of the Kik account "**wildbilk"**, **specified** in Attachment A for the items more fully described in Attachment B.

Respectfully submitted,

/s/ Jonathan Funk
Jonathan Funk
Special Agent
Homeland Security Investigations

Received by reliable electronic means
and sworn and attested to by telephone
on August 11, 2022

JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Kik account **wildbilk** (ESP User ID: **wildbilk_mev**), which is stored at the premises controlled by Kik c/o MediaLab.ai Inc. ("Kik"), a company based in the United States at 1237 7th Street, Santa Monica, California, 90401, which accepts legal process at lawenforcement@kik.com.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Kik c/o MediaLab.ai Inc. ("Kik")

To the extent that the information described in Attachment A is within Kik's possession, custody, or control, including any emails, records, files, logs, or information that has been deleted but is still available to Kik, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Kik is required to disclose the following information to the government:

1. Basic subscriber data, unrestricted by date, associated to the Kik account **wildbilk**;

2. IP addresses associated to the Kik account **wildbilk** from February 22, 2021 to the present;

3. All transactional chat logs associated to the Kik account **wildbilk** from February 22, 2021 to the present;

4. All images and video associated to the Kik account **wildbilk** including the unknown usernames and IP addresses associated to the sender of the images and video from February 22, 2021 to the present;

5. A date-stamped log showing the usernames that Kik account **wildbilk** added and/or blocked from February 22, 2021 to the present;

6. All abuse reports associated with the Kik account **wildbilk** including the unknown usernames from February 22, 2021 to the present;

7. All emails associated with the Kik account **wildbilk** from February 22, 2021 to the present;

8. Registration IP address associated with the Kik account **wildbilk**;

9. User **wildbilk**'s group create log including the creator's username and IP address;

10. User **wildbilk**'s group join logs from February 22, 2021 to the present, including the inviter and invitee username(s) and IP addresses;

11. User **wildbilk**'s group leave logs from February 22, 2021 to the present, including the remover and removed username(s) and IP addresses;

12. User **wildbilk**'s group transactional chat logs from February 22, 2021 to the present, including the senders' IP addresses;

13. User **wildbilk**'s images and videos sent to groups including the sender's and receiver's usernames, and IP addresses associated to the sender of the images and videos from February 22, 2021 to the present.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

The United States intends to seize the following items and information related to violations of 18 U.S.C. § 2422(b) (attempted coercion and enticement of a minor to engage in illegal sexual activity) and 18 U.S.C. § 1470 (attempted transfer of obscene material to a minor), including: :

1. Records, documents, or electronic files identifying the account creator and/or user, and individuals or correspondents using the account to engage in the production, sharing, receipt, collection, or possession of child pornography;

2. "Chat" or messaging transcripts, visual depictions, and materials pertaining to child pornography, child erotica, an interest in such materials, or pertaining to a sexual interest in children, or sexual activity involving children;

3. Records, documents, electronic files, or correspondence pertaining to any minor who is, or appears to be, the subject of any visual depiction of child pornography, child erotica, sexual activity with other minors or adults, or of sexual interest, or that may be helpful in identifying any such minors;

4. Location information associated with the account that may help identify suspects, the account user, or show where events occurred, and who sent, received, possessed or produced child pornography or other evidence of the crime under investigation;

5. Information about the devices used to access the account;

6. EXIF or other metadata about images, documents, correspondence, or other electronic files reflecting a sexual interest in children, or that help identify the device or person who produced, sent, traded, received, or possessed child pornography or that identifies the user of the accounts used to engage in child exploitative acts;

7. Records and information concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members, and/or that advertise, promote, discuss or otherwise involve child pornography;

8. Records pertaining to the means and source of any payments for services (including any credit card or bank account number or digital money transfer account information) related to child pornography, child erotica, an interest in such materials, or pertaining to a sexual interest in children, or sexual activity involving children;

9. Evidence related to any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.